AF
IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Cameron Mashayekhi

Title: APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT

Docket No.: 1565.027US1
Filed: March 3, 2000
Examiner: Matthew E. Heneghan

Serial No.: 09/518,664
Due Date: September 27, 2006
Group Art Unit: 2134

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

X Appeal Brief Under 37 CFR 41.37 (22 pgs.) including authorization to charge Deposit Account 19-0743 in the amount of $500.00 to cover the Appeal Fee..

X Return postcard.

If not provided for in a separate paper filed herewith, Please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Customer Number 21186

By: /Joseph P. Mehrle/
Atty: Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 27 day of September, 2006.

Peter Rebuffoni
Name

Peter
Signature

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Cameron Mashayekhi

Examiner: Matthew E. Heneghan

Serial No.: 09/518,664

Group Art Unit: 2134

Filed: March 03, 2000

Docket: 1565.027US1

Title: APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT

APPEAL BRIEF UNDER 37 CFR § 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

The Appeal Brief is presented in response to the Notice of Panel Decision from Pre-Appeal Brief Review mailed on July 24, 2006 and further in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on July 24, 2006 and received on July 27, 2006, from the Final Rejection of claims 1-20 of the above-identified application, as set forth in the Final Office Action mailed on May 24, 2006.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of $500.00 which represents the requisite fee set forth in 37 C.F.R. § 41.20(b)(2). The Appellant respectfully requests consideration and reversal of the Examiner's rejections of pending claims.

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

TABLE OF CONTENTS

Page

1. REAL PARTY IN INTEREST 2

2. RELATED APPEALS AND INTERFERENCES 3

3. STATUS OF THE CLAIMS 4

4. STATUS OF AMENDMENTS 5

5. SUMMARY OF CLAIMED SUBJECT MATTER 6

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 9

7. ARGUMENT 10

8. SUMMARY 14

CLAIMS APPENDIX 15

EVIDENCE APPENDIX 20

RELATED PROCEEDINGS APPENDIX 21

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, NOVELL, INC.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

The present application was filed on March 3, 2000 with claims 1-14. Claims 15-20 were added in an Amendment filed in response to the non-final Office Action mailed September 11, 2003. A Final Office Action (hereinafter "the Final Office Action") was mailed May 24, 2006. Claims 1-20 stand twice rejected, remain pending, and are the subject of the present Appeal.

4. STATUS OF AMENDMENTS

No amendments have been made subsequent to the Final Office Action dated May 24, 2006.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Some aspects of the present inventive subject matter include, but are not limited to, systems and methods for automatically authenticating a network client. In an aspect of the invention, an authentication system suitable for automatically providing authentication to a user at a client node is presented (FIG. 2 and Specification, page 3 first full paragraph, page 7 first full paragraph and continuing through at least the first full paragraph of page 8). The user provides a user secret (Specification, page 5 second paragraph lines 19-20) and requests access to network resources resident at one or more server nodes in a distributed network system (Specification, page 7 lines 1-3). The authentication system includes: a local application program interface for receiving the user secret, where the local application program interface is in communication with a requested network resource and the client node (FIG. 2 reference numeral 121 and Specification page 8 lines 17-21). The authentication system also includes a cryptography service node having means for providing a common key and algorithm, and having means for providing a client/server session key and algorithm, where the session key is associated with a single session during a single logon of the user and if the session terminates the session key becomes invalid (FIG. 2 reference numeral 125 and Specification page 9 lines 6-12 and page 13 lines 13-20). The authentication system also includes an authentication database in communication with the local application program interface and with the cryptography service node (FIG. 2 reference numeral 103; FIG. 3; and Specification page 8 lines 10-13). The authentication database includes an authentication secret associated with the user (Specification page 8 lines 10-13); means for encrypting the authentication secret using the common key and algorithm (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27); and means for encrypting the common key using the client/server session key and algorithm (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27). The local application program interface sends an encrypted authentication secret, an encrypted common key, and the session key to the client node for use with the requested network resource, and the common key is a shared and same key, and the use occurs during the single session of the user and expires when the single session expires (FIG. 8B, Specification page 18 lines 3-12 and Specification page 13 lines 13-20).

According to another aspect, a method for automatically authenticating a user at a network client node in a distributed network system in response to a user request for access to network resources resident in one or more server nodes is provided (FIGS. 6A-6C and Specification page 12 lines 20-29). A network resource identifier, a network resource policy, and an authentication secret to an authentication database, are provided; the network resource identifier is associated with the requested network resource (FIG. 6A reference block 311 and Specification page 13 lines 21-28). Further, the authentication secret is retrieved in response to the user request, and the authentication secret is associated with the user and with the network resource identifier (FIG. 6C and Specification page 14 lines 19-28). The authentication secret is encrypted with a common key and algorithm (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27). The common key is a shared and same key (Specification page 17 lines 3-18). Also, the common key and algorithm are encrypted with a client/server session key and algorithm (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27). The session key is associated with a single a session of a logon of the user and when the session terminates the session key becomes invalid (Specification page 13 lines 13-20). Moreover, the encrypted authentication secret and the common key are sent to the client node for use by the client during the single session, and the use expires when the single session expires (Specification page 13 lines 13-20).

In still another aspect, a method for authenticating a client to a network resource is presented (FIGS. 6A-6C and 7A-7C). A client receives a request for a network resource and the client is authenticated and a secure session is created (Specification page 9 lines 10-12; Specification page 13 lines 17-20; Specification page 14 lines 23-25; FIG. 6C reference block 325). An authentication secret is created for access to the network resource (FIG. 9B reference block 407 and Specification page 18 line 30 through page 19 line 5. Further, the authentication secret is encrypted within a common key, where the common key is a shared and same key (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27; Specification page 17 lines 3-18). Moreover, the common key is encrypted with a session key associated with the secure session, where the session key becomes invalid when the secure session terminates and where the secure session is associated with a single login session of the client (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27; Specification page 13 lines 13-20). Furthermore, the encrypted common key, the encrypted authentication secret, and the session key are is transmitted to the client for use in accessing the network resource during the single login session, and the use expires when the single login session expires (Specification page 13 lines 13-20).

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellant refers to the appended claims and its legal equivalents for a complete statement of the invention

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-11, 13, 15, 17, 18 and 20 were rejected under 35 USC § 103(a) as being unpatentable over Kahn (U.S. Patent No. 5,818,936) in view of Mashayekhi (U.S. Patent No. 6,401,206) and in further view of Menezes ("Handbook of Applied Cryptology," 1997, pp. 494, 515, and 516).

Claims 12, 14, 16, and 19 were rejected under 35 USC § 103(a) as being unpatentable over Khan in view of Mashayekhi and in further view of Menezes and in still further view of Spies (U.S. Patent No. 5,869,565).

7. ARGUMENT

A) The Applicable Law under 35 U.S.C. §103(a)

To sustain a rejection under 35 U.S.C. 103, references must be cited that teach or suggest all the claim elements. M.P.E.P. § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); *Schenck v. Nortron Corp.*, 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983); *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985); MPEP § 2141.02.

Further, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP § 2143. The Examiner must avoid hindsight. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). The Office Action must further provide specific, objective evidence of record for a finding of a suggestion or motivation to combine reference teachings and must explain the reasoning by which the evidence is deemed to support such a finding. *In re Sang Su Lee*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).

B) Discussion of the rejection of the claims 1-11, 13, 15, 17, 18 and 20 as being unpatentable under 35 USC § 103(a) over Kahn in view of Mashayekhi and in further view of Menezes.

Primarily, the Examiner has relied on Kahn's public key usage to be combined with the notion of a "session key" in the Menezes reference to assert that the independent claims are obvious. The limitations and usages of the session key included in Applicants' independent claims were rejected in the context of citations and explanations to the Kahn reference. Subsequent to that discussion the Examiner asserted that although Kahn discusses public key, the public key could be modified as a session key using the teaching of a session key supplied in Menezes.

Applicants assert that this rejection is improper and cannot be made for a variety of reasons. It is also noted again for purposes of emphasis that mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).

First, a public key and a session key are very different keys and recognized as such in the industry. A session key is temporary and frequently changed. See https://whatis.techtarget.com with key phrase "session key." Session keys are generally used with message communication whereas public keys are used for identities. Public keys are longer and require more processing. See http://en.wikipedia.org/wiki/Main_Page key phrases "session key" and "public key." In fact, in the Final Office Action the Examiner acknowledged that there is "a clear difference between public keys and session keys." See Final Office Action, Mailed May 24, 2006, page 5, item 4 and last paragraph. Thus, it appears that there is no dispute with the Examiner that public keys and session keys are in fact clearly different from one another, as the Examiner has already made this admission on record.

The Examiner claims that the Menezes reference establishes a session key via a public key algorithm so this is sufficient to tie the two together and use session key in the context of public key taught and disclosed in Kahn. The Examiner did not cite where this is indicated in the Menezes reference. The Menezes reference appears to be a handbook on cryptology, the section the Examiner only discusses session keys and motivation for session keys it does not tie them into public key algorithms as the Examiner has asserted. However, even assuming that it did, this is irrelevant as to whether the rejection is proper because the fact that a public key algorithm is used to generate a session key (as the Examiner asserted without reference to such a teaching within Menezes) does not change the fact that the teaching supplied in Kahn is exclusively for a public key arrangement and not a session key arrangement. The Examiner is asserting that a session key could be generated from a public key algorithm but this is irrelevant because the teachings in Kahn are directed to using a "public key" and not using a "session key."

Second, to combine references there must be some reasonable expectation of success and the intended functions of the cited references cannot be lost. If Kahn were modified with a session key teaching of Menezes its teaches would be lost. The Board's attention is directed to Kahn column 8 lines 20-29. Here it can be clearly seen that a digital identity and public key are created once in the identity's life cycle. The Examiner asserts that because the identity is modifiable it demonstrates that it may be temporary. Applicants directs the Board's attention to column 8 lines 30-36 where it is clear that the public key remains unchanged in such a situation.

The Kahn reference cannot be changed or be modified so as to make its teaching and usage of public key equivalent to that of a session key because in so doing the Kahn reference would fail in its intended function of providing permanency to identities and public keys of identities. Moreover, such a modification would not have a reasonable expectation of success because the public key in Kahn would become temporary and not permanent. Applicants respectfully assert that one of ordinary skill in the art would not have been motivated to combine a general handbook on cryptology of Menezes with the specific teachings of the Kahn public key to change the public key in Kahn to a session key because in so doing the very benefits and stated purposes of the intended benefits and functions of Kahn would be lost. Kahn seeks to create a biometric or unique signature that individuals can apply to documents to identify them selves; this is directly opposed to teachings associated with temporary keys and identifiers. Consequently, Kahn teaches away from Menezes and the two references are not combinable.

Accordingly, Applicants respectfully assert that the proposed combination is improper and should be withdrawn and the claims allowed. Applicants respectfully request an indication of the same.

C) Discussion of the rejection of the claims 12, 14, 16, and 19 as being unpatentable under 35 USC § 103(a) over Khan in view of Mashayekhi and in further view of Menezes and in still further view of Spies (U.S. Patent No. 5,869,565).

Applicants note that these claims are dependent from the independent claims, thus these claims are allowable if the independent claims are allowed. Applicants respectfully assert that in view of the comments supplied above these claims are allowable and respectfully request an indication of the same.

8. SUMMARY

For the reasons argued above, the independent claims were not properly rejected under § 103(a) as being unpatentable over Mashayekhi in view of Menezes.

It is respectfully submitted that the art cited does not render the independent claims obvious and that the claims are patentable over the cited art. Therefore, reversal of the rejections and allowance of the pending claims are respectfully requested.

Respectfully submitted,

CAMERON MASHAYEKHI

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date __September 27, 2006________ By Joseph P. Mehrle /
Joseph P. Mehrle
Reg. No. 45,535

<u>CERTIFICATE UNDER 37 CFR 1.8:</u> The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 27 day of September 2006.

Peter Rebuffoni
Name

Signature

CLAIMS APPENDIX

1. An authentication system suitable for automatically providing authentication to a user at a client node, the user providing a user secret and requesting access to network resources resident at one or more server nodes in a distributed network system, said authentication system comprising:

a local application program interface for receiving the user secret, said local application program interface in communication with a requested network resource and the client node;

a cryptography service node including means for providing a common key and algorithm, and means for providing a client/server session key and algorithm, wherein the session key is associated with a single session during a single logon of the user and if the session terminates the session key becomes invalid; and

an authentication database in communication with said local application program interface and with said cryptography service node, said authentication database including

an authentication secret associated with the user;

means for encrypting said authentication secret using said common key and algorithm; and

means for encrypting said common key using said client/server session key and algorithm;

wherein the local application program interface sends an encrypted authentication secret, an encrypted common key, and the session key to the client node for use with the requested network resource, and wherein the common key is a shared and same key, and wherein the use occurs during the single session of the user and expires when the single session expires.

2. The authentication system of claim 1 further comprising means for encrypting and decrypting said authentication secret using a secret store key and algorithm.

3. The authentication system of claim 1 further comprising,

a network resource identifier associated with said requested network resource; and

a network policy associated with the user and with said network resource identifier.

4. The authentication system of claim 3 wherein said authentication database further comprises,

a second network resource identifier associated with a second network resource;

a second authentication secret associated with the user; and

a second network policy associated with the user and with said second network resource identifier.

5. The authentication system of claim 4 wherein said authentication database further comprises means for encrypting and decrypting said second authentication secret using said secret store key and algorithm.

6. The authentication system of claim 4 wherein said authentication database further comprises means for encrypting and decrypting said second authentication secret using a second secret store key and algorithm.

7. The authentication system of claim 1 wherein said cryptography service further comprises means for generating an authentication secret from the user secret.

8. The authentication system of claim 1 wherein said common key comprises a symmetric key.

9. A method for automatically authenticating a user at a network client node in a distributed network system in response to a user request for access to network resources resident in one or more server nodes, said authentication method comprising the steps of:

providing a network resource identifier, a network resource policy, and an authentication secret to an authentication database, said network resource identifier associated with the requested network resource;

retrieving said authentication secret in response to said user request, said authentication secret associated with the user and with said network resource identifier;

encrypting said authentication secret with a common key and algorithm, wherein the common key is a shared and same key;

encrypting said common key and algorithm with a client/server session key and algorithm, wherein the session key is associated with a single a session of a logon of the user and when the session terminates the session key becomes invalid; and

sending said encrypted authentication secret and said encrypted common key to the client node for use by the client during the single session, and wherein the use expires when the single session expires.

10. The method of claim 9 further comprising the steps of:

decrypting said encrypted common key using said client/server session key;

decrypting said encrypted authentication secret using said decrypted common key and algorithm; and

providing said decrypted authentication secret to the requested network resource.

11. The method of claim 9 further comprising the step of accessing said network resource policy prior to said step of retrieving said authentication secret, said network resource policy associated with the user and with said network resource identifier.

12. The method of claim 9 further comprising the steps of:

obtaining a list of client algorithms supported by the client node;

obtaining a list of server algorithms supported by the server node;

comparing said list of client algorithms with said list of server algorithms so as to determine the strongest algorithm common to both said list of client algorithms and said list of server algorithms; and

using said strongest algorithm as said common key and algorithm.

13. The method of claim 9 wherein said common key comprises a symmetric key.

14. The method of claim 9 further comprising the steps of:
negotiating the strongest common algorithm between server and client node; and
using said strongest algorithm as said client/server session key and algorithm.

15. A method for authenticating a client to a network resource, comprising:
receiving a client request for a network resource;
authenticating the client and creating a secure session;
creating an authentication secret for access to the network resource;
encrypting the authentication secret within a common key, wherein the common key is a shared and same key;
encrypting the common key with a session key associated with the secure session, wherein the session key becomes invalid when the secure session terminates and wherein the secure session is associated with a single login session of the client; and
transmitting to the client the encrypted common key, the encrypted authentication secret, and the session key for use in accessing the network resource during the single login session, and wherein the use expires when the single login session expires.

16. The method of claim 15 further comprising, determining a strongest encryption and decryption algorithm supported by the client when encrypting the authentication secret within the common key.

17. The method of claim 15 further comprising receiving, by the network resource, a decrypted version of the authentication secret from the client and authenticating the client for access to the network resource based on the decrypted authentication secret.

18. The method of claim 15 further comprising associating policies with the authentication secret, wherein the policies define access rights of the client to the network resource.

19. The method of claim 15 negotiating with the client encryption and decryption algorithms for use in encrypting the authentication secret and the common key.

20. The method of claim 15 associating the authentication secret with the client and the network resource and housing the association in a secret store for additional secure sessions established by the client.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.